EXHIBIT A

(Complete State Court Record)

49D01-2305-PL-021530
Marion Superior Court 1
Filed: 5/26/2023 3:24 PM
Clerk
Marion County, Indiana

INDIANA COMMERCIAL COURT

STATE OF INDIANA)
) SS:
COUNTY OF MARION)

IN THE MARION SUPERIOR COURT 1

CAUSE NO. _____

KAITLIN LAMARR, Individually, and on behalf of all others similarly situated,

Plaintiff

v.

GOSHEN HEALTH SYSTEM, INC. D/B/A GOSHEN HEALTH,

Defendant

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, KAITLIN LAMARR, Individually, and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant, GOSHEN HEALTH SYSTEM, INC. D/B/A GOSHEN HEALTH, and alleges, upon personal knowledge as to their own actions and on information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendant's outrageous, illegal, and widespread practice of disclosing the confidential Personally Identifying Information[1] ("PII") and/or Protected Health Information[2] ("PHI") (collectively referred to as "Private Information")

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created,

of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google, LLC ("Google"), Crazy Egg Inc. ("Crazy Egg"), StackAdapt, Inc. ("StackAdapt"), Trade Desk, CallTrackingMetrics, LLC ("CallTrackingMetrics"), Simplifi Holdings, LLC ("Simplifi"), and possibly others ("the Disclosure").

2. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace and denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system.

3. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no

---

collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Goshen Health is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

4. Goshen Health is an Indiana-based, regional healthcare with a 110 year history.[3] It is a major healthcare provider, operating nearly healthcare clinics across four counties (Elkhart, Kosciusko, LaGrange, and Noble), as well as the Goshen Hospital and the Goshen physician network of family medicine and specialty providers.[4] Goshen Health prides itself on its reputation "[n]ationally recognized, award-winning leader in innovative cancer treatment" and describes its vision for itself as a "trust partner for care."[5]

5. Defendant encourages its patients to use its website, https://www.goshenhealth.org/, (the "Website") and its various web-based tools and services, which allow patients to search for physicians, locate healthcare facilities, learn about specific health conditions and treatment options, pay bills, sign up for classes and events, and more (collectively referred to as the "Online Platforms").

6. Despite its unique position as a massive and trusted healthcare provider, Goshen Health knowingly configured and implemented into its Website devices known as "pixels," which then collected and transmitted patients' information to third parties. This included information and communicated by patients through Defendant's sensitive and presumptively confidential Online Platforms.

7. When Plaintiff and Class Members used Defendant's Online Platforms, they thought were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendant embedded pixels from Facebook, Google, Crazy Egg, StackAdapt, Trade Desk,

---

[3] Goshen Health Fact Sheet, GOSHEN HEALTH, https://goshenhealth.com/health-library/pr-goshen-health-fact-sheet (last visited May 24, 2023).
[4] *Id.*
[5] *Id.*

CallTrackingMetrics, and Simplifi into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties.

8. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[6] When a person visits a website with an embedded pixel, the pixel tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[7] Then, the pixel transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[8]

9. Among the pixels Defendant embedded into its Website and Online Platforms is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a visitor's device, including their IP address, and the pages viewed.[9] When configured, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[10] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[11]

---

[6] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[7] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[8] *Id.*
[9] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[10] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[11] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

10. Operating as designed and as implemented by Defendant, the Meta Pixel allowed Defendant to unlawfully disclose Plaintiff and Class Members' private health information alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook, without Plaintiff's and Class Members' authorization or knowledge.

11. In addition to its use of the Meta Pixel to spy on and transmit Plaintiff's and Class Members' Private Information, Facebook encourages and recommends use of its Conversions Application Programming Interface ("CAPI").[12]

12. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[13, 14]

13. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[15]

---

[12] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[13] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[14] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

[15] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

14. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly.

15. Defendant utilized data from these trackers to market its services and bolster its profits. Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

16. The information that Defendant's Meta Pixel and CAPI sent to Facebook can include the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including, for example, the type of medical treatment sought, the individual's healthcare provider or health condition, or registration details for a class or event.

17. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Meta Pixel and CAPI. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

18. In addition to the Facebook Pixel and CAPI, Defendant has installed Facebook Events, Google Tag Manager, Crazy Egg, StackAdapt, Trade Desk, CallTrackingMetrics, and Simplifi. On information and belief, these trackers operate similarly to the Meta Pixel and transmit

a website user's Private Information to unauthorized third parties.

19. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Personal Health Information or other confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

20. Neither Plaintiff nor any Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook, Google, Crazy Egg, StackAdapt, Trade Desk, CallTrackingMetrics, and Simplifi, or any other third parties uninvolved in their treatment.

21. Despite willfully and intentionally incorporating tracking technology, including the Meta Pixel, potentially CAPI, and other tracking technology, into its Website and servers, Goshen Health has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with third parties like Facebook, Google, Crazy Egg, StackAdapt, Trade Desk, CallTrackingMetrics, and Simplifi.

22. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook and other third parties as they communicated their confidential PHI with their healthcare provider via the Website and Online Platforms.

23. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

24. Defendant owed common law, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and Private Information safe, secure, and confidential.

25. According to information and belief, Goshen Health utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data

analytics, attract new patients, and generate sales.

26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

27. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiff's and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

28. Plaintiff seeks to remedy these harms and bring causes of action for (I) Negligence, (II) Invasion of Privacy, (III) Breach of Implied Contract, (IV) Unjust Enrichment, (V) Breach of Fiduciary Duty, (VI) Violation of the Indiana Deceptive Consumer Sales Act, and (VII) Violation of the Indiana Wiretapping Act.

PARTIES

29. Plaintiff, Kaitlin Lamarr, is a natural person and a resident and citizen of Indiana where she intends to remain, with a principal residence in Goshen, Indiana, Elkhart County. She has been a patient of Goshen Health since 2018, and she is a victim of Defendant's unauthorized

Disclosure of Private Information.

30. Defendant Goshen Health System, Inc. d/b/a Goshen Health ("Goshen Health" or "Defendant") is a non-profit corporation organized and existing under the laws of Indiana and with its principal place of business in Elkhart County at 200 High Park Avenue, Goshen, Indiana, 46256-4810.

JURISDICTION AND VENUE

31. This Court has jurisdiction over the subject matter of this action by virtue of Indiana Rule Trial Procedure 4.4 because Goshen Health operates and provides services within the state of Indiana.

32. This case is eligible for the Indiana Commercial Court docket under Indiana Commercial Court Rules 2 and 4.

COMMON FACTUAL ALLEGATIONS

A. Background

33. Goshen Health, headquartered in Goshen, Indiana, is "[a] comprehensive healthcare network" offering a full range of medical services, from primary care and emergency services to cancer treatment and other specialties.[16] Its flagship facility, Goshen Hospital, is a 103-bed hospital (also located in Goshen, Indiana)[17] that provides emergency and rehabilitative services to the surrounding area.

34. Goshen Hospital also operates nearly forty other clinics, including the Business Health Advantage clinic, Goshen Center for Cancer Care, Goshen Heart & Vascular Center (two locations), Goshen Home Care & Hospice, Goshen Home Medical, Goshen Imaging Center, Goshen Orthopedics, Goshen Physicians Center for Weight Reduction, Goshen Physicians

[16] About Us, GOSHEN HEALTH, https://goshenhealth.com/about-us (last visited May 23, 2023).
[17] *Id.*

Endocrinology, Goshen Physicians Family Medicine (thirteen locations), Goshen Physicians Gastroenterology, Goshen Physicians Internal Medicine, Goshen Physicians OB/GYN, Goshen Physicians Parkway at 17, Goshen Physicians Pediatrics, Goshen Physicians Sleep & Allergy Medicine, Goshen Physicians Urology, Goshen Rehabilitation Services, Goshen Retreat Women's Health Center, Goshen Sleep Disorders Center, Goshen Surgery Center, Goshen Wound & Hyperbaric Center, NeuroCare Center Goshen Physicians, and Urgent Care Goshen Physicians.[18]

35. Additionally, Goshen Health operates its own network of physicians who offer medical care across a broad range of specialties.[19]

36. Goshen Health serves many of its patients through its Website and Online Platforms. Defendant promotes the convenience and comprehensive functionality of its Online Platforms. It encourages its patients to use its Online Platforms to search for physicians, locate healthcare facilities, learn about specific health conditions and treatment options, pay bills, sign up for classes and events, and more.

37. In furtherance of that goal and to increase the success of its advertising and marketing and sales, Defendant purposely installed the Meta Pixel and trackers on its Website and Online Platforms. In doing so, Defendant surreptitiously shared patients' private and protected communications, including those containing Plaintiff's and Class Members' Private Information, with Facebook and other third parties.

38. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

[18] Goshen Health Fact Sheet, GOSHEN HEALTH https://goshenhealth.com/health-library/pr-goshen-health-fact-sheet (last visited May 24, 2023).
[19] https://goshenhealth.com/find-a-doctor

39. As Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[20]

40. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

41. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

42. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[21] Businesses that want to target customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[22]

43. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type of actions they take."[23] When a user accesses a webpage that is hosting the Meta Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent

---

[20] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

[21] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[22] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

[23] Retargeting, META, https://www.facebook.com/business/goals/retargeting.

to Facebook—traveling from the user's browser to Facebook's server.

44. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as the "Find a Doctor" page).

45. The Meta Pixel's primary purpose is for marketing and ad targeting and sales generation.[24]

46. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[25]

47. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers ***include IP addresses***, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[26]

---

[24] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[25] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).
[26] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

48. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[27]

49. Facebook likewise benefits from the data received from the Meta Pixel and uses the data to serve targeted ads and identify users to be included in such targeted ads.

ii. Defendant's method of transmitting Plaintiff's and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

50. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

51. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

52. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[28]

---

[27] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

[28] "Cookies are small files of information that a web server generates and sends to a web browser . . . .

53. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

54. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information (such as Defendant's "Find a Doctor" page). The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

55. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

56. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

57. Defendant's implementation of the Meta Pixel is source code that acted much like a traditional wiretap, intercepting and transmitting communications intended only for Defendant.

58. Separate from the Meta Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendant's Website, the account holder's unique Facebook ID is

---

Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

sent to Facebook, along with the intercepted communication, allowing Facebook to identify the patient associated with the Private Information it has intercepted.

59. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade. Facebook's workaround is its Conversions API tool, which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from the entity's server to Facebook's server.

60. Conversions API "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[29] Thus, the entity receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

61. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

62. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[30] Thus, if an entity implemented the Meta Pixel in in accordance with Facebook's documentation, it is also reasonable to infer that it implemented the Conversions API tool on its Website.

---

[29] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).
[30] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

63. The third parties to whom a website transmits data through pixels and other tracking technology do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user relating to the user's communications. Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (i.e., to bolster profits).

64. Accordingly, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer its patients' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the patients' communications to hidden third parties like Facebook.

65. In this case, Defendant employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

66. Consequently, when Plaintiff and Class Members visited Defendant's website and communicated their Private Information, it is simultaneously intercepted and transmitted to Facebook.

67. Goshen Health employed other trackers from Google, Crazy Egg, StackAdapt, Trade Desk, CallTrackingMetrics, and Simplifi, which, on information and belief, likewise transmitted Plaintiff's and the Class Members' Private Information to third parties without Plaintiff's and Class Members' knowledge or authorization.

iii. Defendant Violated its own Privacy Policy

68. Goshen Health maintains and is covered under its Privacy Policy, maintained on Defendant's Website.[31]

[31] *See* Privacy Policy, GOSHEN HEALTH, https://goshenhealth.com/health-library/privacy-policy (last visited May 23, 2023), **attached as Exhibit A.**

69. Defendant's Privacy Policy provides, "**THIS NOTICE DESCRIBES HOW YOUR PROTECTED HEALTH INFORMATION MAY BE USED AND DISCLOSED, AND WHAT RIGHTS YOU MAY HAVE TO ACCESS YOUR PROTECTED HEALTH INFORMATION.**"[32]

70. Defendant's Privacy Policy further states that

> This Notice of Privacy Practices describes how Goshen Hospital may use and disclose your protected health information to carry out treatment, for payment, for healthcare operations and for other purposes permitted or required by law. This Notice also describes certain rights that you may have to access your protected health information. Goshen Hospital is required to abide by the terms of this Notice of Privacy Practices.[33]

71. In its Privacy Policy, Defendant goes on to acknowledge, represent, and promise that "Goshen Hospital **will not disclose your protected health information for marketing purposes** or the sale of protected health information."[34]

72. Moreover, Defendant promises that "[i]ndividuals will receive notifications of their unsecured protected health information that is breached."[35]

73. On information and belief, Defendant does not maintain a separate website privacy policy.

74. Despite its representations, Defendant did, in fact, disclose Plaintiff's and Class Members' protected health information to Facebook and other third parties for the purpose of marketing its services and increasing profit and sales. This was a violation of Defendant's Privacy Policy.

75. For example, if a patient visits Defendant's website and clicks "Goshen Center for

---

[32] *Id.*
[33] *Id.*
[34] *Id.* (emphasis added).
[35] *Id.*

Cancer Care" under Defendant's "Care Services" page, the patient's browser sends a request to Defendant's server requesting that it load the webpage. Then, Meta Pixel sends secret instructions back to the individual's browser, causing the browser to imperceptibly record the patient's communication with Goshen Health and transmit it to Facebook's servers, alongside personally identifying information (e.g., the patient's IP address).

76. Facebook then processes data received from the Meta Pixel to build marketing and data profiles on particular individuals.

77. On information and belief, Goshen Health also disclosed Plaintiff's and Class Members' protected health information to Google, Crazy Egg, StackAdapt, Trade Desk, CallTrackingMetrics, and Simplifi, through its use of other third-party trackers, Facebook and other third parties for the purpose of marketing its services and increasing its profits and sales. This too violated Defendant's Privacy Policy.

78. Similar to the way Facebook links a website visitor's activities with that visitor's identity to build marketing profiles, Google and other companies process data gleaned from tracking technology to build marketing and data profiles on particular individuals.

79. In this way, Defendant disclosed personally identifiable information connected with private information about their medical conditions and treatment with Facebook and other third parties, thereby revealing Plaintiff's and Class Member's protected health information to Facebook and other third parties, in violation of its Privacy Policy.

80. On information and belief, Defendant exchanged Plaintiff's and Class Members' protected health information with third parties for improved marketing and data analytics. This also violated Defendant's Privacy Policy.

81. Defendant could have chosen not to use the Meta Pixel and other tracking

technology, or it could have configured its trackers to limit the information that it communicated to third parties, but it chose not to. Instead, it intentionally took advantage of these trackers' features and functions, resulting in the Disclosure of Plaintiff's and Class Members' Private Information.

82. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant Goshen Health to disclose their Private Information or intercept their communications. Plaintiff was never provided with any written notice that Defendant discloses its patients' Protected Health Information, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's Protected Health Information to Facebook and possibly other unauthorized entities.

83. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

84. Furthermore, Defendant never disclosed to Plaintiff or Class Members that their "unsecured protected health information . . . [wa]s breached." This also was a violation of Defendant's Privacy Policy.

85. By law, Plaintiff and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. Goshen Health deprived Plaintiff and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others; and (3) undertook this pattern of conduct without authorization and without notifying Plaintiff and

Class Members of the Disclosure.

B. Plaintiff's Experience

86. Plaintiff Kaitlin Lamarr is a patient of Defendant and received healthcare services from Goshen Health clinics and physicians. She relied on Goshen Health's Online Platforms to communicate confidential patient information.

87. Plaintiff Ms. Lamarr accessed Defendant's Online Platforms at Defendant's direction and encouragement. Ms. Lamarr reasonably expected that her online communications with Goshen Health were confidential, solely between herself and Goshen Health, and that, as such, those communications would not be transmitted to or intercepted by a third party.

88. Plaintiff Ms. Lamarr provided her Private Information to Defendant and trusted that the information would be safeguarded according to Goshen Health's privacy policies and the law.

89. When Ms. Lamarr used Defendant's Online Platforms, Goshen Health sent her Private Information to Facebook, and possibly other third parties, through its use of the Meta Pixel and other tracking technology.

90. Pursuant to the process described herein, Goshen Health assisted Facebook (and possibly others) with intercepting Ms. Lamarr's confidential communications and Private Information. Goshen Health facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization, and without notifying Plaintiff that her Private Information was compromised.

91. Health disclosed Ms. Lamarr's Private Information to Facebook and other third parties for the exclusive reason of marketing its services and increasing profit.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

92. In June 2020, after promising users that app developers would not have access to

data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[36] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

93. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[37]

94. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[38] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook,

---

[36] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.
[37] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[38] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[39]

95. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[40]

96. Furthermore, in June 2022, an investigation by The Markup[41] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[42] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[43] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[44]

97. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article

---

[39] *Id.*
[40] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[41] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[42] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[43] *Id.*
[44] *Id.*

found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[45]

98. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[46]

99. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[47]

D. Defendant Violated HIPAA Standards

100. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[48]

101. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

102. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

> health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[49]

103. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[50]

104. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[51]

105. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[52]

106. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking**

---

[49] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[50] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[51] *See* U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.

[52] *Id.*

> **technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [53]

107. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel is a violation of HIPAA Rules.

E. Defendant Violated Industry Standards

108. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

109. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Goshen Health and its physicians.

110. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

111. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information

[53] *Id.* (emphasis in original) (internal citations omitted).

> they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

112. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

F. Plaintiff's and Class Members' Expectation of Privacy

113. At all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for commercial marketing and sales purposes, unrelated to patient care.

G. IP Addresses are Personally Identifiable Information

114. Defendant also disclosed and otherwise assisted Facebook and potentially others with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other tracking technologies.

115. An IP address is a number that identifies the address of a device connected to the Internet.

116. IP addresses are used to identify and route communications on the Internet.

117. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

118. Facebook tracks every IP address ever associated with a Facebook user.

119. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

120. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

121. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

H. Defendant Was Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures

122. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was marketing and profits.

123. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing on its platform.

124. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

125. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

I. Plaintiff's and Class Members' Private Information Had Financial Value

126. Plaintiff's data and Private Information has economic value. Facebook regularly

uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

127. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is due to increase; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

128. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[54]

129. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[55]

TOLLING, CONCEALMENT, AND ESTOPPEL

130. The applicable statutes of limitation have been tolled as a result of Goshen Health's knowing and active concealment and denial of the facts alleged herein.

131. Goshen Health seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing users with no indication that their Website usage

[54] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.
[55] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

was being tracked and transmitted to third parties. Goshen Health knew that its Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, and likely other third parties, including Google, YouTube, CrazyEgg, Simpli.fi, Cloudflare, MangoDB, Hotjar, Trade Desk

132. Plaintiff and Class Members could not with due diligence have discovered the full scope of Goshen Health's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel or any other tracking technology.

133. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Goshen Health's illegal interception and disclosure of Plaintiff's Private Information has continued unabated through the present. What's more, RMA was under a duty to disclose the nature and significance of their data collection practices but did not do so. RMA is therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

134. Plaintiff brings this statewide class action on behalf of themselves and on behalf of other similarly situated persons.

135. The statewide Class that Plaintiff seeks to represent is defined as

> **All Indiana citizens whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

136. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

137. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

138. Numerosity: Class Members are so numerous that joinder of all members is impracticable. On information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class is apparently identifiable within Defendant's records.

139. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include

a. whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' Private Information;

b. whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Private Information;

f. whether and when Defendant actually learned of the Disclosure;

g. whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

h. whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

i. whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

j. whether Defendant adequately addressed and fixed the vulnerabilities that permitted the Disclosure to occur; and

k. whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiff's and Class Members' Private Information.

140. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use and incorporation of Meta Pixel and other tracking technology.

141. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

142. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of

the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

143. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

144. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish

the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

145. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

146. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

147. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful disclosure and failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding Disclosure, and Defendant may continue to act unlawfully as set forth in this Complaint.

148. Further, Defendant has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

149. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendant breached a legal duty to Plaintiff and Class Members to exercise

due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. whether Defendant breached the implied contract;

f. whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

h. whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information; and

i. whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

150. Plaintiff realleges and incorporates the above allegations as if fully set forth herein.

151. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that

occurred.

152. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

153. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiff's and Class Members' Private Information.

154. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way of data harvesting, advertising, and increased sales.

155. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

156. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

157. Defendant's breach of its common-law duties to exercise reasonable care and its

failures and negligence actually and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's negligence. These injuries are ongoing, imminent, immediate, and continuing.

COUNT II
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

158. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

159. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and Online Platforms and the communications platforms and services therein.

160. Plaintiff and Class Members communicated PHI and PII—confidential, sensitive, private information—that they intended for only Defendant to receive and that they understood Defendant would keep private.

161. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion and their private affairs and concerns.

162. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations, and Privacy Policy. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is highly offensive to the

reasonable person.

163. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

164. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

165. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

166. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

167. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

168. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

169. As a condition of receiving medical care from Defendant, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received. In so doing, Plaintiff and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Policy and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

170. Implicit in the agreement between Goshen Health and its patients, Plaintiff and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

171. Goshen Health had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Goshen Health.

172. Goshen Health had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

173. Additionally, Goshen Health implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

174. Plaintiff and Class Members fully performed their obligations under the implied contract with Goshen Health. Goshen Health did not. Plaintiff and Class Members would not have provided their confidential Private Information to Goshen Health in the absence of their implied contracts with Goshen Health and would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from Goshen Health.

175. Goshen Health breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to an unauthorized third party.

176. Goshen Health's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

177. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

178. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

180. This claim is pleaded solely in the alternative to Plaintiff's Breach of Implied Contract claim.

181. Plaintiff and Class members conferred a monetary benefit upon Goshen Health in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendant in the form of monetary compensation.

182. Plaintiff and Class Members would not have used Goshen Health's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Private Information to third parties.

183. Goshen Health appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class members.

184. As a result of Goshen Health's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without unreasonable data privacy and security practices and

procedures that they received.

185. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members themselves. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

186. Goshen Health should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Disclosure alleged herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

187. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

188. A relationship existed between Plaintiff and the Class, on the one hand, and Defendant, on the other, in which Plaintiff and the Class put their trust in Defendant to protect the Private Information of Plaintiff and the Class, and Defendant accepted that trust.

189. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, their Private Information.

190. Defendant's breach of fiduciary duty was a legal cause of injury-in-fact and damage to Plaintiff and the Class.

191. But for Defendant's breach of fiduciary duty, the injury-in-fact and damage to Plaintiff and the Class would not have occurred.

192. Defendant's breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

193. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT V
VIOLATION OF THE INDIANA DECEPTIVE CONSUMER SALES ACT
(On Behalf of Plaintiff and the Class)

194. Plaintiff re-alleges and incorporates the preceding paragraphs of this Complaint as if fully set forth herein.

195. The purposes and policies of the Indiana Deceptive Consumer Sales Act (the "DCSA"), Indiana Code § 24-5-0.5-1 to -12, are to:

(1) simplify, clarify, and modernize the law governing deceptive and unconscionable consumer sales practices;
(2) protect consumers from suppliers who commit deceptive and unconscionable consumer sales practices; and
(3) encourage the development of fair consumer sales practice.

Ind. Code § 24-5-0.5-1(b).

196. The General Assembly has instructed courts to construe the DCSA liberally to promote these purposes and policies. Ind. Code § 24-5-0.5-1(a).

197. Goshen Health is a "supplier" as defined in the DCSA because it is a seller or other person who regularly engages in or solicits consumer transactions, which are defined to include sales of personal property, *services*, and intangibles that are primarily for a personal, familial, or household purpose, such as those at issue in this action. Ind. Code § 24-5-0.5-2(1), (3) (emphasis added).

198. The DCSA provides that "[a] supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act,

omission, or practice by a supplier is a violation of [the DCSA] whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." Ind. Code § 24-5-0.5-3(a).

199. An "incurable deceptive act" is a "deceptive act done by a supplier as part of a scheme, artifice, or device with the intent to defraud or mislead. Ind. Code § 24-5-0.5-2(a)(8).

200. The DCSA further provides:

> Without limiting the scope of subsection (a) the following acts, and the following representations as to the subject matter of a consumer transaction, made orally, in writing, or by electronic communication, by a supplier, are deceptive acts:
>
> a. That such subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have
> b. That such subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not . . . .

Ind. Code § 24-5-0.5-3

201. Goshen Health committed deceptive acts, including but not limited to the following.

a. Goshen Health encouraged its patients to use Goshen Health's Online Platform while representing its commitment to protecting the privacy of the Personal Information. Defendant also promised patients that it will never sell its patients' protected health information or share it for marketing purposes.

b. Despite these representations, Goshen Health disclosed to Facebook and other third parties information relating to Plaintiff's and Class Members' medical treatment, without their knowledge, consent, or authorization, as part of a scheme, artifice or device with the intent to mislead patients.

c. Plaintiff and Class Members relied on Goshen Health's representations in using

Goshen Health's Online Platform and thought they were communicating only with their trusted healthcare provider.

d. By installing and implementing the Meta Pixel, Defendant knew or reasonably should have known it intercepted and transmitted Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to Facebook. Likewise, by installing or implementing CAPI, Defendant knew or reasonably should have known that it recorded on its servers and transmitted to Facebook Plaintiff's and Class Member's confidential communications.

202. Goshen Health's violations were willful and were done as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore are incurable deceptive acts under the DCSA.

203. The DCSA provides that "[a] person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater. The court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (i) three (3) times the actual damages of the consumer suffering the loss; or (ii) one thousand dollars ($1,000). Ind. Code § 24-5-0.5-4(a).

204. The DCSA provides that "[a]ny person who is entitled to bring an action under subsection (a) on the person's own behalf against a supplier for damages for a deceptive act may bring a class action against such supplier on behalf of any class of persons of which that person is a member . . . ." Ind. Code § 24-5-0.5-4(b).

205. Had Plaintiff and members of the Classes been aware that their Private Information would be transmitted to unauthorized third parties, they would not have entered into

such transactions and would not have provided payment or confidential medical information to Goshen Health.

206. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the DCSA, Plaintiff and Class Members have suffered damages for which Defendant is liable.

207. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the DCSA. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, *inter alia*, actual damages, treble damages, attorneys' fees, and injunctive relief.

COUNT VI
Violation of the Indiana Wiretapping Act
(On Behalf of Plaintiff and the Class)

208. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

209. The Indiana Wiretapping Act (the "IWA") states that "a person who knowingly or intentionally intercepts a communication in violation of this article commits unlawful interception, a Level 5 felony." Ind. Code § 35-33.5-5-5. The term "includes the intentional recording or acquisition of communication through the use of a computer[.]" *Id.*

210. For purposes of the IWA, "interception" is the "intentional recording or acquisition of the contents of an electronic communication by a person other than a sender or receiver of that communication, without the consent of the sender or receiver, by means of any instrument, device, or equipment under this article." Ind. Code § 35-31.5-2-176.

211. Defendant Goshen Health intentionally recorded and/or acquired Plaintiff's and Class Members' electronic communications, without the consent of the Plaintiff and Class

Members, using the Meta Pixel and other trackers.

212. Defendant intentionally recorded and/or acquired Plaintiff's and Class Members' electronic communications for the purpose of disclosing those communications to third parties, including Facebook, without the knowledge, consent, or written authorization of Plaintiff or Class Members.

213. Under the IWA, "[a] person whose communications are intercepted, disclosed, or used in violation of this article . . . has a civil cause of action against a person who intercepts, discloses, uses, or procures another person to intercept, disclose, or use a communication," and is entitled to recover from that person

a. the greater of:
    i. actual damages;
    ii. liquidated damages computed at a rate of one hundred dollars ($100) each day for each day of violation; or
    iii. one thousand dollars ($1,000).
b. court costs (including fees).
c. punitive damages, when determined to be appropriate by the court.
d. reasonable attorney's fees.

Ind. Code § 35-33.5-5-4.

214. Goshen Health is a "person" under the IWA. Ind. Code § 35-31.5-2-234.

215. The devices used in this case, include, but are not limited to

a. those to which Plaintiff's and Class Members' communications were disclosed;

b. Plaintiff's and Class Members' personal computing devices;

c. Plaintiff's and Class Members' web browsers;

d. Plaintiff's and Class Members' browser-managed files;

e. the Meta Pixel;

f. internet cookies;

g. other pixels, trackers, and/or tracking technology installed on Defendant's Website

and/or server;

h. Defendant's computer servers;

i. third-party source code utilized by Defendant; and

j. computer servers of third parties (including Facebook).

216. Defendant aided in the interception of communications between Plaintiff and Class Members and Defendant that were redirected to and recorded by third parties without the Plaintiff's or Class Members' consent.

217. Under the IWA, Plaintiff and the Class Members are entitled to recover actual damages, but not less than liquidated damages at a rate of $100 a day for each day of the violation or one thousand dollars ($1,000), whichever is greater, punitive damages, reasonable attorney's fees, and court costs.

218. In addition to statutory damages, Defendant's breach caused Plaintiff and Class Members the following damages:

a. sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the doctor-patient relationship;

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiff's and Class Members'

personal information.

219. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Ms. Lamarr, Individually, and on behalf of all others similarly situated, prays for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;

B. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

D. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. for an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. for an award of punitive damages, as allowable by law;

H. for an award of attorneys' fees under the IWA, DCSA, the common fund doctrine, and any other applicable law;

I. costs and any other expenses, including expert witness fees incurred by Plaintiff in connection with this action;

J. pre- and post-judgment interest on any amounts awarded; and

K. such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, pursuant to Indiana Trial Rule 38(B), hereby demands a trial by jury on all issues so triable.

Dated: May 26, 2023

Respectfully submitted,

/s/ Lynn A. Toops

Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
Mary Kate Dugan (No. 37623-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

Goshen Health

(/)

(tel://15743641000)

Español (/Health-Library/Privacy-Policy?lang=es-mx)

FOOTER

Privacy policy

THIS NOTICE DESCRIBES HOW YOUR PROTECTED HEALTH INFORMATION MAY BE USED AND DISCLOSED, AND WHAT RIGHTS YOU MAY HAVE TO ACCESS YOUR PROTECTED HEALTH INFORMATION. PLEASE REVIEW IT CAREFULLY.

Goshen Hospital believes your health information is personal and is committed to protecting the privacy of the health information it creates or receives about you. Goshen Hospital has a professional and legal obligation to respect your confidentiality.

"Protected health information" is health information or other individually identifiable information such as demographic data, that may identify you. Protected health information is information about your past, present or future physical or mental health or condition related to healthcare services.

This Notice of Privacy Practices describes how Goshen Hospital may use and disclose your protected health information to carry out treatment, for

payment, for healthcare operations and for other purposes permitted or required by law. This Notice also describes certain rights that you may have to access your protected health information. Goshen Hospital is required to abide by the terms of this Notice of Privacy Practices.

The terms of this Notice may change at any time. The new Notice will apply to all protected health information acquired after it goes into effect. Upon your request, Goshen Hospital will provide you with any historical Notice of Privacy Practices or you may obtain the most current copy.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION THAT DO NOT REQUIRE YOUR AUTHORIZATION

Your protected health information may be used and disclosed by those involved in your care and treatment for the purpose of providing healthcare services to you. Your protected health information may also be used and disclosed to obtain payment for services rendered and to support the operations of Goshen Hospital. The following list, by way of example rather than limitation, explains certain uses and disclosures of your protected health information that Goshen Hospital is permitted to make.

TREATMENT

Goshen Hospital will use and disclose your protected health information to provide, coordinate or manage your healthcare and any related services. This includes the coordination or management of your healthcare with another provider. For example, Goshen Hospital may disclose your protected health information, as minimally necessary, to a home health agency that provides care to you.

Goshen Hospital will also disclose health information to physicians or other healthcare providers who may be treating you. For example, your protected health information may be provided to a physician to whom you have been referred to ensure that the physician has the necessary information to treat you.

In addition, Goshen Hospital may disclose your protected health information from time-to-time to another physician or healthcare provider (e.g., specialist or laboratory) who, at the request of your physician becomes involved in your care by providing assistance with your healthcare diagnosis or treatment. As another example, a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process.

Goshen Hospital participates in certain Health Information Exchanges or Organizations (HIEs or HIOs). For example, Goshen Hospital participates in the Indiana Health Information Exchange (IHIE) and Indiana Network for Patient Care (INPC), which helps to make your protected health information available to other healthcare providers who may need access to it in order to provide care or treatment to you.

PAYMENT

Goshen Hospital may use and disclose your protected health information as necessary to obtain payment for healthcare services. For example: (1) to make a determination of eligibility or coverage for insurance benefits, (2) review services provided to you for medical necessity and to undertake utilization-review activities and (3) approve or pay for recommended healthcare.

HEALTHCARE OPERATIONS

Goshen Hospital may use or disclose your protected health information in order to support our business activities. These activities include, but are not limited to, quality assessment activities, employee review activities, training of medical students, licensing, and conducting or arranging for other business activities. Goshen Hospital may share your protected health information with "business associates" or thirdparty organizations which perform services such as billing or transcription services on behalf of Goshen Hospital. Goshen Hospital has written contracts with its business associates to protect the privacy of your protected health information, and business associates are also required by law to comply with the same privacy and security requirements that apply to Goshen Hospital.

Goshen Hospital may use and disclose your protected health information to tell you about appointments and other matters related to your care. We may contact you by mail, telephone or e-mail. We may leave voice messages at the telephone number you provide to us, and we may respond to your emails.

Goshen Hospital may use and disclose your protected health information to tell you about possible treatment options, new services or alternatives that may be relevant to your healthcare.

FUNDRAISING ACTIVITIES

Goshen Hospital may use protected health information to contact you in an effort to raise money for its operations. It may disclose protected health information to a foundation related to Goshen Hospital so that it may raise money to support Goshen Hospital; you may request, in writing, not to be contacted for this purpose.

HOSPITAL DIRECTORY

Goshen Hospital may include limited information about you in the hospital directory while you are a patient. This information may include your name, location in the hospital and your general condition (e.g., fair or stable). This directory information may be released to people who ask for you by name so that they may generally know how you are doing. If you do not want this information shared, please let us know. Also, your religious affiliation may be given to a member of the clergy even if they do not ask for you by name.

INDIVIDUALS INVOLVED IN YOUR CARE OR PAYMENT FOR YOUR CARE

Unless you indicate otherwise, Goshen Hospital may disclose to a relative, a close friend or other person you identify, a portion of your protected health information which directly relates to your healthcare. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary for your healthcare, if, based on our professional judgment, we determine that it is in your best interest. We may disclose protected health information to notify or assist in notifying a family member or personal representative (or any other person who is responsible for your

care) of your location, general condition or death. Finally, we may disclose your protected health information to an authorized public or private entity to assist in disaster-relief efforts.

RESEARCH

Goshen Hospital performs medical research. Goshen Hospital may disclose your protected health information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure, among other things, the privacy of protected health information. Goshen Hospital may release information about you to researchers who need to know how many patients have a specific health issue in preparation for proposed research. If a doctor caring for you believes you may be interested in, or may benefit from, a research study, your physician and the research review committee will designate someone to contact you. This individual will see if you are interested in the study, provide you with more information and give you the opportunity to participate or to decline further contact.

TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

Goshen Hospital may use and disclose protected health information about you when necessary to prevent a serious threat to your health and safety, or the health and safety of another person or the public. However, any disclosure would only be to someone who is able to help prevent the threat.

ORGAN AND TISSUE DONATION

Goshen Hospital may release protected health information to organizations that handle organ procurement or organ, eye or tissue transplantation, or to an organ-donation bank as minimally necessary to facilitate organ or tissue donation and transplantation.

WORKERS' COMPENSATION

Goshen Hospital may release protected health information about you for workers' compensation or similar programs that provide benefits for work-related injuries or illnesses.

PUBLIC HEALTH RISKS AND PATIENT SAFETY ISSUES

Goshen Hospital may disclose protected health information to a public health authority that is permitted by law to receive the information for public health activities. For example, disclosures may be made for the purposes of preventing or controlling disease, injury or disability; to report births and deaths; to report reactions to medications or problems with products; and to notify people of recalls of products that they may be using.

COMMUNICABLE DISEASES

Goshen Hospital may disclose or use your protected health information to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition, and to comply with state-mandatory disease reporting, such as cancer registries.

ABUSE OR NEGLECT

Goshen Hospital may disclose your protected health information to a public health authority authorized by law to receive reports of child abuse or neglect, and to notify the appropriate government authority if Goshen Hospital believes a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure as required or authorized by law.

HEALTH OVERSIGHT ACTIVITIES

Goshen Hospital may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, inspections and licensure. These activities are necessary for the government to monitor the healthcare system, government benefit programs and compliance with civil-rights laws.

FOOD AND DRUG ADMINISTRATION (FDA)

Goshen Hospital may disclose your protected health information to a person or company required by the Food and Drug Administration for the purpose of managing the quality, safety or effectiveness of FDA-regulated products or activities, which include: reporting adverse events, product defects or problems, biologic product deviations; tracking products; enabling product recalls; making repairs or replacements; or to conduct post-marketing surveillance, as required.

LEGAL PROCEEDINGS

Goshen Hospital may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly

authorized) or in certain conditions in response to a subpoena, discovery request or other lawful process.

LAW ENFORCEMENT

Goshen Hospital may disclose protected health information for certain law-enforcement purposes, such as: in response to a court order, subpoena, warrant, summons or similar process; to identify or locate a suspect, fugitive, material witness or missing person; about the victim of a crime, if under certain limited circumstances, we are unable to obtain the person's agreement; about a death we believe may be the result of criminal conduct; about criminal conduct at the hospital; and, in emergency circumstances, to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

CORONERS, MEDICAL EXAMINERS AND FUNERAL DIRECTORS

Goshen Hospital may release protected health information to a coroner or medical examiner, for example, to identify a deceased person or determine the cause of death. We may also release protected health information about patients of the hospital to funeral directors as necessary to carry out their duties.

MILITARY ACTIVITY AND NATIONAL SECURITY

Goshen Hospital may use or disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military-command authorities, for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits or to foreign military authority if you are a member of that foreign

military service. Protected health information may also be disclosed to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the president or others legally authorized.

INMATES

If you are an inmate of a correctional institution or under the custody of a law enforcement official, Goshen Hospital may release protected health information about you to the correctional institution or law enforcement official. This release would be necessary for the institution to provide you with healthcare, to protect your health and safety or the health and safety of others or for the safety and security of the correctional institution.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION THAT DO REQUIRE YOUR AUTHORIZATION

As described above, Goshen Hospital may use or disclose your protected health information to third parties for treatment, payment, healthcare operations and when permitted or required by law. Goshen Hospital will not disclose your protected health information for marketing purposes or the sale of protected health information. In addition, certain disclosures of

your psychotherapy notes, mental health records and drug and alcohol abuse treatment records may require your prior written authorization.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

RIGHT TO INSPECT AND COPY

You have the right to inspect and obtain an electronic or paper copy of your protected health information that may be used to make decisions about your care. This includes medical and billing records, but may not include psychotherapy notes. To inspect and obtain a copy of your protected health information, you must submit your request in writing to the Goshen Hospital Health Information Management department. If you request a copy of the information, Goshen Hospital may charge a fee for the cost of copying, mailing or other supplies associated with your request.

Goshen Hospital may deny your request to inspect and copy records in some limited circumstances. If you are denied access to protected health information, you may request that the denial be reviewed. Another licensed healthcare professional chosen by Goshen Hospital will review your request and the denial. The person conducting the review will not be the person who denied your request. Goshen Hospital will comply with the outcome of the review.

RIGHT TO AMEND

You have a right to request an amendment of the health information that Goshen Hospital has in our records. Your request for an amendment must be made in writing, including a reason for the request and submitted to the Goshen Hospital Performance Improvement department. Goshen Hospital may deny a request for an amendment if it is not in writing and does not include a reason to support the request or requests for amendment of information that: was not created by Goshen Hospital; is not part of the protected health information kept by Goshen Hospital; is not part of the information which you would be permitted to inspect and copy; or is accurate and complete.

RIGHT TO RECEIVE NOTIFICATION

Individuals will receive notifications of their unsecured protected health information that is breached.

RIGHT TO AN ACCOUNTING OF DISCLOSURES

You have the right to request an accounting of disclosures. This is a list of disclosures Goshen Hospital has made of your protected health information, excluding disclosures for treatment, payment, healthcare operations or disclosures you authorized in writing. To request an accounting of disclosures, submit your request in writing and include the specific time period to Goshen Hospital Health Information Management department. Goshen Hospital will not list disclosures made earlier than six years before your request.

The first accounting of disclosure in a 12-month period is free. Additional

accounting of disclosures may cost a fee; you will be notified in advance of any cost involved so that you may choose to withdraw or modify your request before incurring a cost.

RIGHT TO REQUEST RESTRICTIONS

You have the right have the right to request a restriction on the ways your protected health information is used or disclosed. To request a restriction, submit your request in writing to the Goshen Hospital Privacy Counsel office. The request should include what information you want to limit, whether you want to limit use or disclosure, or both, and to whom you want the limits to apply – for example, disclosures to your spouse. Goshen Hospital is not required to agree to your request. If we do agree, we will comply with your restriction unless the information is needed to provide emergency medical treatment.

Goshen Hospital will agree to restrict disclosures of your health information to your health insurance plan for payment and healthcare operations purposes (not for treatment) if the disclosure pertains solely to a healthcare item or service for which you paid in full.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATION

You have the right to request that Goshen Hospital communicate with you about healthcare matters in a certain way or at a certain location. For example, you can request that you are only contacted at work or at a specific address. Such requests should be made in writing to the Goshen Hospital Performance Improvement department and should specify how or where you wish to be contacted. Goshen Hospital will accommodate all reasonable requests.

RIGHT TO A PAPER COPY OF THIS NOTICE

You have the right to a paper copy of this Notice of Privacy Practices, even if you have agreed to receive this Notice electronically. You may also find a copy of this Notice on the Goshen Health website, at www.GoshenHealth.com/Privacy.

OTHER USES OF PROTECTED HEALTH INFORMATION

Other uses and disclosures of your protected health information not covered by this Notice or allowed by law will be made only with your written permission. If you provide permission to use or disclose protected health information, you may revoke that permission, in writing, at any time. If you revoke your permission, Goshen Hospital will no longer use or disclose protected health information about you for the reasons covered by your written authorization. Goshen Hospital is unable to take back any disclosures it may have already made with your permission.

CHANGES TO THIS PRIVACY NOTICE

Goshen Hospital reserves the right to change this Notice and to make the revised or changed Notice effective for protected health information we already have about you, as well as any information we receive in the future. The revised Notice of Privacy Practices will be posted on our website at www.GoshenHealth.com/Privacy; request that a revised or historical copy be sent to you in the mail or obtain one at the time of an appointment at Goshen Hospital.

QUESTIONS OR COMPLAINTS

If you believe Goshen Hospital has violated your privacy rights, you may file a complaint with Goshen Hospital Privacy Counsel office or with the Secretary of the Department of Health and Human Services. You will not be penalized for filing a complaint. To file a complaint with Goshen Hospital, please submit a complaint in writing to the Goshen Hospital Performance Improvement department.

If you have further questions about this Notice of Privacy Practices, please contact the Goshen Hospital Privacy Officer as follows:

Chris Hutfless
Chief Legal, Human Resources and Compliance Officer

Goshen Hospital

200 High Park Ave.

Goshen, IN 46526

(574) 364-2898 (tel://15743642898)

chutfless (mailto:chuftless@goshenhealth.com)@goshenhealth.com (mailto:chutfless@goshenhealth.com)

Goshen Hospital Health Information Management Department Release of Information

200 High Park Ave.

Goshen, IN 46526.

Telephone: (574) 364-1074 (tel://15743641074)

Goshen Hospital Privacy Officer

Goshen Hospital

200 High Park Ave.

Goshen, IN 46526

Telephone: (574) 364-2898 (tel://15743642898)

Goshen Hospital Marketing

Goshen Hospital

200 High Park Ave.

Goshen, IN 46526

Telephone: (574) 364-2915 (tel://15743642915)

Goshen Hospital Performance Improvement Department

Goshen Hospital

200 High Park Ave.

Goshen, IN 46526

Telephone: (574) 364-2353 (tel://15743642353)

Office for Civil Rights

U.S. Department of Health and Human Services

233 N. Michigan Ave., Suite 240

Chicago, IL 60601 dhhs.gov

dhhs.gov (https://www.hhs.gov/)

Goshen Health complies with applicable Federal civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability or sex.

ATTENTION: If you speak Spanish, language assistance services, free of charge, are available to you. Call **1** (tel://15743641000)**(574) 364-1000** **(tel://15743641000)** (TTY: 711 or **1 (800) 743-3333** (tel://18007433333) to be connected with Relay Indiana).

Updated 3/30/21

(https://www.youtube.com/channel/UCfPGW9cDRZQiPQ-tygwKhA)

Find A Doctor (/find-a-doctor)

Locations (/locations)

Patients & Visitors (/patient-information)

For Providers (/about-us/provider-quick-guide)

Health Library (/health-library)

Care Services (/care-services)

Jobs (/jobs)

For Employers (/about-us/business-health-advantage)

Give (/about-us/goshen-health-foundation)

About Us (/about-us)

Newsroom (/about-us/newsroom)

Partners (/health-library/partners)

Price Transparency (/patient-information/estimates-financial-assistance)

Legal (/health-library/goshen-health-nondiscrimination-notice)

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT 1
	) SS:	
COUNTY OF MARION	)	CAUSE NO. _____

KAITLIN LAMARR, Individually, and on behalf of all others similarly situated,	)
Plaintiff	)
v.	)
GOSHEN HEALTH SYSTEM, INC. D/B/A GOSHEN HEALTH,	)
Defendant	)

APPEARANCE BY ATTORNEY IN CIVIL CASE

Party Classification:
Initiating _X___ Responding ____ Intervening_____

1. The undersigned attorney and all attorneys listed on this form now appear in this case for the following party member(s): Plaintiff Kaitlin Lamarr, individually and on behalf of all others similarly situated

2. Applicable attorney information for service as required by Trial Rule 5(B)(2) and for case information as required by Trial Rules 3.1 and 77(B) is as follows:

Name: Lynn A. Toops — Atty No: 26386-49
Address: Cohen & Malad, LLP — Phone: (317) 636-6481
One Indiana Square, Suite 1400 — Fax: (317) 636-2593
Indianapolis, IN 46204 — E-mail: ltoops@cohenandmalad.com

Name: Amina A. Thomas — Atty No: 34451-49
Address: Cohen & Malad, LLP — Phone: (317) 636-6481
One Indiana Square, Suite 1400 — Fax: (317) 636-2593
Indianapolis, IN 46204 — E-mail: athomas@cohenandmalad.com

Name: Mary Kate Dugan — Atty No: 37623-49
Address: Cohen & Malad, LLP — Phone: (317) 636-6481
One Indiana Square, Suite 1400 — Fax: (317) 636-2593
Indianapolis, IN 46204 — E-mail: mdugan@cohenandmalad.com

3. There are other party members: Yes __ No _X_ (If yes, list on continuation page)

4. ***If first initiating party filing this case:*** the Clerk is requested to assign this case the following Case Type under Administrative Rule 8(b)(3): __n/a_____

5. I will accept service by FAX at the above-noted number: Yes ___ No _X

6. This case involves support issues. Yes ___ No _X
(If yes, supply social security numbers for all family members on continuation page)

7. There are related cases: Yes ___ No _X__ (If yes, list on continuation page)

8. This form has been served on all other parties. Certificate of Service is attached: Yes_X_ No_

9. Additional information required by local rule: none

Dated: May 26, 2023

Respectfully submitted,

/s/ Lynn A. Toops
Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
Mary Kate Dugan (No. 37623-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

CERTIFICATE OF SERVICE

I certify that a copy of this document was filed electronically on May 26, 2023. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

/s/ Lynn A. Toops
Lynn A. Toops

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT 1
	) SS:	
COUNTY OF MARION	)	CAUSE NO. _____

KAITLIN LAMARR, Individually, and on behalf of all others similarly situated,	)
Plaintiff	)
v.	)
GOSHEN HEALTH SYSTEM, INC. D/B/A GOSHEN HEALTH,	)
Defendant	)

NOTICE IDENTIFYING COMMERCIAL COURT DOCKET CASE

The undersigned states that this case is a Commercial Court Docket Case eligible for assignment to the Commercial Court Docket pursuant to Rule 2 of the Commercial Court Rules.

Pursuant to Rule 4 of the Commercial Court Rules, the undersigned requests that the Clerk of Court assign the case to the Commercial Court Docket.

Dated: May 26, 2023

Respectfully submitted,

/s/ *Lynn A. Toops*
Lynn A. Toops
Amina A. Thomas
Mary Kate Dugan
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)

STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
Gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I certify that a copy of this document was filed electronically on May 26, 2023. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

/s/ Lynn A. Toops
Lynn A. Toops

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT 1
	) SS:	
COUNTY OF MARION	)	CAUSE NO. _____

KAITLIN LAMARR, Individually, and on behalf of all others similarly situated,	)
Plaintiff	)
v.	)
GOSHEN HEALTH SYSTEM, INC. D/B/A GOSHEN HEALTH,	)
Defendant	)

SUMMONS

To: Goshen Health System, Inc.
c/o Chris Hutfless, Registered Agent
200 High Park Avenue
Goshen, IN 46526

You are hereby notified that you have been sued by the person named as plaintiffs and in the Court indicated above.

The nature of the suit against you is stated in the complaint, which is attached to this Summons. It also states the relief sought or the demand made against you by the plaintiffs.

An answer or other appropriate response in writing to the complaint must be filed either by you or your attorney within twenty (20) days, commencing the day after you receive this Summons, (or twenty-three (23) days if this Summons was received by mail), or a judgment by default may be rendered against you for the relief demanded by the plaintiffs.

If you have a claim for relief against the plaintiffs arising from the same transaction or occurrence, you must assert it in your written answer.

If you need the name of an attorney, you may contact the Indianapolis Bar Association Lawyer Referral Service (317-269-2222), or the Marion County Bar Association Lawyer Referral Service (317-269-2000).

5/30/2023

Dated:_____ _____(Seal)
CLERK, SUPERIOR COURT

(The following manner of service of summons is hereby designated.)

__X_ Registered or certified mail.
_____ Service at place of employment, to-wit: _____
_____ Service on individual – (Personal or copy) at above address.
__X__ Service on agent. (Specify) **c/o Chris Hutfless, Registered Agent, 200 High Park Avenue, Goshen, IN 46526**
_____ Other service. (Specify)

MARION COUNTY COURTS SEAL INDIANA

s/ Lynn A. Toops
Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
Mary Kate Dugan (No. 37623-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

CLERK'S CERTIFICATE OF MAILING

I hereby certify that on the _____ day of _____, 2023, I mailed a copy of this Summons and a copy of the Complaint, to the defendant, by _____ mail, requesting a return receipt, at the address furnished by the plaintiff.

_____
Clerk of the Circuit/Superior
Court of Marion County

Dated: _____, 2023 By: _____
Deputy

RETURN ON SERVICE OF SUMMONS BY MAIL

I hereby certify that the attached return receipt was received by me showing that the Summons and a copy of the Complaint, mailed to defendant, was accepted by the defendant on the ____ day of _____, 2023.

I hereby certify that the attached return receipt was received by me showing that the Summons and a copy of the Complaint was returned not accepted on the _____ day of_____, 2023.

I hereby certify that the attached return receipt was received by me showing that the Summons and a copy of the Complaint, mailed to defendant was accepted by _____ _____ on behalf of said defendant on the ____ day of _____, 2023.

_____
Clerk of the Circuit/Superior
Court of Marion County

Dated: _____, 2023

By: _____
Deputy

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT
	) SS:	
MARION COUNTY	)	CAUSE NO. 49D01-2305-PL-021530

KAITLYN LAMARR, individually, and on behalf of all others similarly situated,

Plaintiff

v.

GOSHEN HEALTH SYSTEM, INC. d/b/a GOSHEN HEALTH,

Defendant.

APPEARANCE BY ATTORNEYS IN A CIVIL CASE

1. The party on whose behalf this form is being filed is:

Initiating ___ Responding **X** Intervening ___ ; and

the undersigned attorney and all attorneys listed on this form now appear in this case for the following parties:

Name of party **Defendant, Goshen Health System, Inc. d/b/a Goshen Health**

Address of party *(see Question # 5 below if this case involves a protection from abuse order, a workplace violence restraining order, or a no-contact order)*

c/o Bose McKinney & Evans LLP

Telephone # of party c/o Bose McKinney & Evans LLP

(List on a continuation page additional parties this attorney represents in this case.)

2. Attorney information for service as required by Trial Rule 5(B)(2)

Philip R. Zimmerly
Attorney No. 30217-06

Tyler J. Moorhead
Attorney No. 34705-73

BOSE MCKINNEY & EVANS LLP
111 Monument Circle, Suite 2700
Indianapolis, IN 46204
Phone: (317) 684-5000
Fax: (317) 684-5173

PZimmerly@boselaw.com
TMoorhead@boselaw.com

IMPORTANT: Each attorney specified on this appearance:

(a) certifies that the contact information listed for him/her on the Indiana Supreme Court Roll of Attorneys is current and accurate as of the date of this Appearance;

(b) **acknowledges that all orders, opinions, and notices from the court in this matter that are served under Trial Rule 86(G) will be sent to the attorney at the email address(es) specified by the attorney on the Roll of Attorneys regardless of the contact information listed above for the attorney**; and

(c) understands that he/she is solely responsible for keeping his/her Roll of Attorneys contact information current and accurate, see Ind. Admis. Disc. R. 2(A).

Attorneys can review and update their Roll of Attorneys contact information on the Courts Portal at http://portal.courts.in.gov.

3. This is a **PL** case type as defined in administrative Rule 8(B)(3).

4. This case involves child support issues. Yes ____ No **X** *(If yes, supply social security numbers for all family members on a separately attached document filed as confidential information on **light green paper**. Use Form TCM-TR3.1-4.)*

5. This case involves a protection from abuse order, a workplace violence restraining order, or a no – contact order. Yes ____ No **X** *(If Yes, the initiating party must provide an address for the purpose of legal service but that address should not be one that exposes the whereabouts of a petitioner.)* The party shall use the following address for purposes of legal service:

_____ Attorney's address
_____ The Attorney General Confidentiality program address (contact the Attorney General at 1-800-321-1907 or e-mail address is **confidential@atg.state.in.us)**.
_____ Another address (provide) _____

6. This case involves a petition for involuntary commitment. Yes ____ No **X**

If Yes above, provide the following regarding the individual subject to the petition for involuntary commitment:

(a) Name of the individual subject to the petition for involuntary commitment if it is not already provided in #1 above:

_____

(b) State of Residence of person subject to petition: _____

(c) At least one of the following pieces of identifying information:

(i) Date of Birth _____

(ii) Driver's License Number _____

State where issued _____ Expiration date _____

(iii) State ID number _____

State where issued _____ Expiration date _____

(iv) FBI number _____

(v) Indiana Department of Corrections Number _____

(vi) Social Security Number is available and is being provided in an attached confidential document Yes ____ No ____

7. There are related cases: Yes ____ No **X** *(If yes, list on continuation page.)*

8. Additional information required by local rule:

_____

9. There are other party members: Yes ____ No **X** *(If yes, list on continuation page.)*

10. This form has been served on all other parties and Certificate of Service is attached:

Yes **X** No ___

Dated: June 23, 2023.

/s/ Philip R. Zimmerly

Philip R. Zimmerly (#30217-06)
Tyler J. Moorhead (#34705-73)
BOSE McKINNEY & EVANS LLP
111 Monument Circle, Suite 2700
Indianapolis, IN 46204
T: (317) 684-5000
F: (317) 684-5173
pzimmerly@boselaw.com
tmoorhead@boselaw.com

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on June 23, 2023, a copy of the foregoing was filed electronically. Notice of this filing was served on the following counsel by operation of the Indiana electronic filing system. Parties may access this filing through that system.

Lynn A. Toops
Amina A. Thomas
Mary Kate Dugan
COHEN AND MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

/s/ Philip R. Zimmerly
Philip R. Zimmerly

4598085

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT
	) SS:	
MARION COUNTY	)	CAUSE NO. 49D01-2305-PL-021530

KAITLYN LAMARR, individually, and on behalf of all others similarly situated,

Plaintiff

v.

GOSHEN HEALTH SYSTEM, INC. d/b/a GOSHEN HEALTH,

Defendant.

DEFENDANT'S MOTION FOR AUTOMATIC ENLARGEMENT OF TIME TO ANSWER OR OTHERWISE RESPOND TO THE COMPLAINT

Defendant Goshen Health System Inc. d/b/a Goshen Health ("Defendant"), pursuant to Ind. Trial Rule 6(B)(1) and Marion County LR49-TR5 Rule 203(D), moves this Court for an automatic 30-day enlargement of time to respond to Plaintiff's Class Action Complaint and Jury Demand ("Complaint"), and states as grounds therefore:

1. The Complaint was filed with this Court on May 26, 2023, and served on Defendant on June 5, 2023.

2. Defendant's answer or other responsive pleading is due no later than June 26, 2023, which time has not yet expired.

3. Defendant moves this Court for an automatic 30-day enlargement of time to respond to Plaintiff's Complaint, which shall expire on July 26, 2023.

4. No prior enlargements of time have been requested.

WHEREFORE, Defendant, The Methodist Hospitals, by counsel, respectfully requests the Court to automatically enlarge the time within which it must respond to Plaintiff's Complaint, for a period of 30 days, to and including July 26, 2023.

Respectfully submitted,

/s/ Philip R. Zimmerly
Philip R. Zimmerly (#30217-06)
Tyler J. Moorhead (#34705-73)
BOSE McKINNEY & EVANS LLP
111 Monument Circle, Suite 2700
Indianapolis, IN 46204
T: (317) 684-5000
F: (317) 684-5173
pzimmerly@boselaw.com
tmoorhead@boselaw.com

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on June 23, 2023, a copy of the foregoing was filed electronically. Notice of this filing was served on the following counsel by operation of the Indiana electronic filing system. Parties may access this filing through that system.

Lynn A. Toops
Amina A. Thomas
Mary Kate Dugan
COHEN AND MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

/s/ Philip R. Zimmerly
Philip R. Zimmerly

4598088

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT
	) SS:	
MARION COUNTY	)	CAUSE NO. 49D01-2305-PL-021530

KAITLYN LAMARR, individually, and on behalf of all others similarly situated,

Plaintiff

v.

GOSHEN HEALTH SYSTEM, INC. d/b/a GOSHEN HEALTH,

Defendant.

ORDER

This matter having come before the Court on the *Motion for Automatic Enlargement of Time to Answer Complaint* filed by Defendant, Goshen Health System Inc. d/b/a Goshen Health, and the Court, being fully advised of all factual matters in this cause, now finds that the motion should be GRANTED, and it is accordingly ORDERED that Defendant shall respond to Plaintiff's Complaint on or before **July 26, 2023**.

Dated: 6/23/2023

Heather A. Welch

Judge, Marion County Superior Court

Distribution:

Lynn A. Toops, Esq.
Amina A. Thomas, Esq.
Mary Kate Dugan, Esq.

Philip R. Zimmerly, Esq.
Tyler J. Moorhead, Esq.

Kaitlin Lamarr v. Goshen Health System, Inc. d/b/a Goshen Health

Case Number	49D01-2305-PL-021530
Court	Marion Superior Court 1 Commercial Court (Provisional)
Type	PL - Civil Plenary
Filed	05/26/2023
Status	05/26/2023 , Pending (active)

Parties to the Case

Defendant Goshen Health System, Inc. d/b/a Goshen Health

Attorney
Philip Richard Zimmerly
#3021706, Lead, Retained

Bose McKinney & Evans LLP
111 Monument Circle, Suite 2700
Indianapolis, IN 46204
317-684-5000(W)

Attorney
Tyler John Moorhead
#3470573, Retained

111 Monument Circle Suite 2700
Bose McKinney & Evans LLP
Indianapolis, IN 46204
317-684-5000(W)

Plaintiff Lamarr, Kaitlin

Attorney
Lynn Antoinette Toops
#2638649, Lead, Retained

One Indiana Square
Suite 1400
Indianapolis, IN 46204
317-636-6481(W)

Attorney
Amina Anne Thomas
#3445149, Retained

Cohen & Malad, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
317-636-6481(W)

Chronological Case Summary

05/26/2023	**Case Opened as a New Filing**	
05/30/2023	**Complaint/Equivalent Pleading Filed**	
	Class Action Complaint and Jury Demand	
	Filed By:	Lamarr, Kaitlin
	File Stamp:	05/26/2023
05/30/2023	**Appearance Filed**	
	Notice of Appearance of Lynn A. Toops, Amina A. Thomas and Mary Kate Dugan	
	For Party:	Lamarr, Kaitlin
	File Stamp:	05/26/2023

05/30/2023 **Commercial Court Identifying Notice**
Notice Identifying Commercial Court Docket Case

Filed By: Lamarr, Kaitlin
File Stamp: 05/26/2023

05/30/2023 **Subpoena/Summons Filed**
Summons to Defendant Goshen Health System, Inc. d/b/a Goshen Health

Filed By: Lamarr, Kaitlin
File Stamp: 05/26/2023

06/23/2023 **Appearance Filed**
Appearance for Defendant

For Party: Goshen Health System, Inc. d/b/a Goshen Health
File Stamp: 06/23/2023

06/23/2023 **Motion for Enlargement of Time Filed**
Motion for Automatic Enlargement of Time

Filed By: Goshen Health System, Inc. d/b/a Goshen Health
File Stamp: 06/23/2023

06/23/2023 **Order Granting Motion for Enlargement of Time**

Judicial Officer: Welch, Heather A
Order Signed: 06/23/2023

06/24/2023 **Automated ENotice Issued to Parties**
Order Granting Motion for Enlargement of Time ---- 6/23/2023 : Amina Anne Thomas;Lynn Antoinette Toops;Philip Richard Zimmerly;Tyler John Moorhead

Financial Information

* Financial Balances reflected are current representations of transactions processed by the Clerk's Office. Please note that any balance due does not reflect interest that has accrued – if applicable – since the last payment. For questions/concerns regarding balances shown, please contact the Clerk's Office.

Lamarr, Kaitlin
Plaintiff

Balance Due (as of 07/03/2023)
0.00

Charge Summary

Description	Amount	Credit	Payment
Court Costs and Filing Fees	157.00	0.00	157.00

Transaction Summary

Date	Description	Amount
05/30/2023	Transaction Assessment	157.00
05/30/2023	Electronic Payment	(157.00)